[EGY FEJLESZTŐI TEREPMUNKA KÉZIKÖNYV]

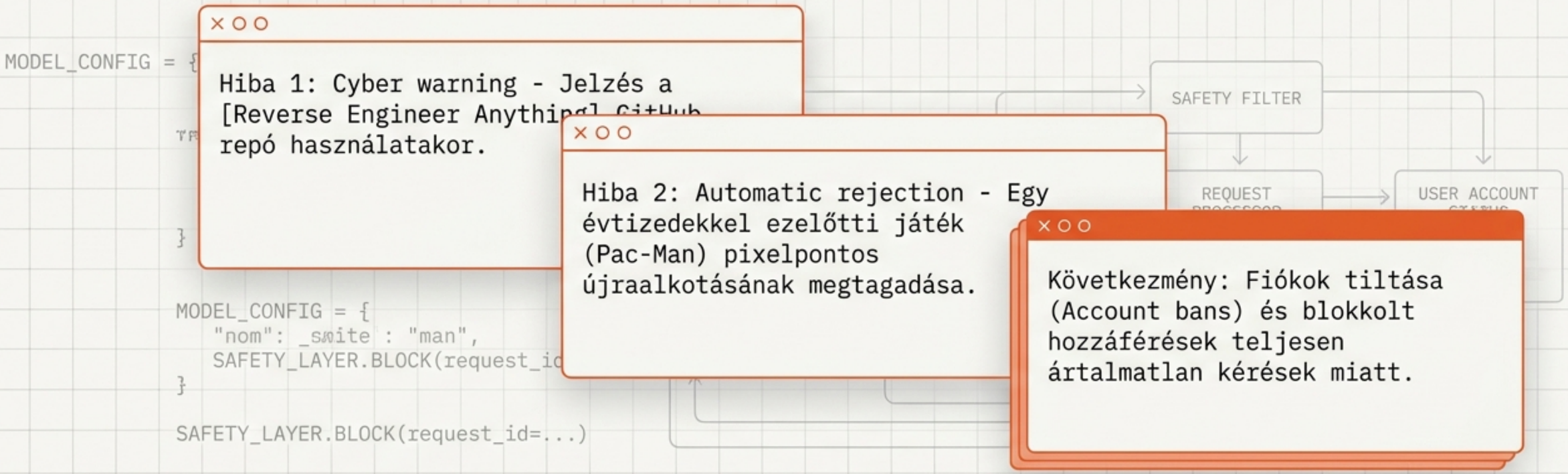
A korlátlan mesterséges intelligencia gyakorlati útmutatója

Hogyan kerüljük meg a főáramú AI modellek korlátozásait a cenzúrázatlan ökoszisztéma kihasználásával.

Gemini Notebook

A főáramú AI modellek egyre gyakrabban tagadnak meg ártalmatlan kéréseket.

Bár az AI asszisztensek egyre okosabbak, a beépített biztonsági korlátok gyakran akadályozzák a mindennapi fejlesztői munkát.



Gemini Notebook

A cenzúrázatlan modellek visszaadják a teljes irányítást a felhasználónak.

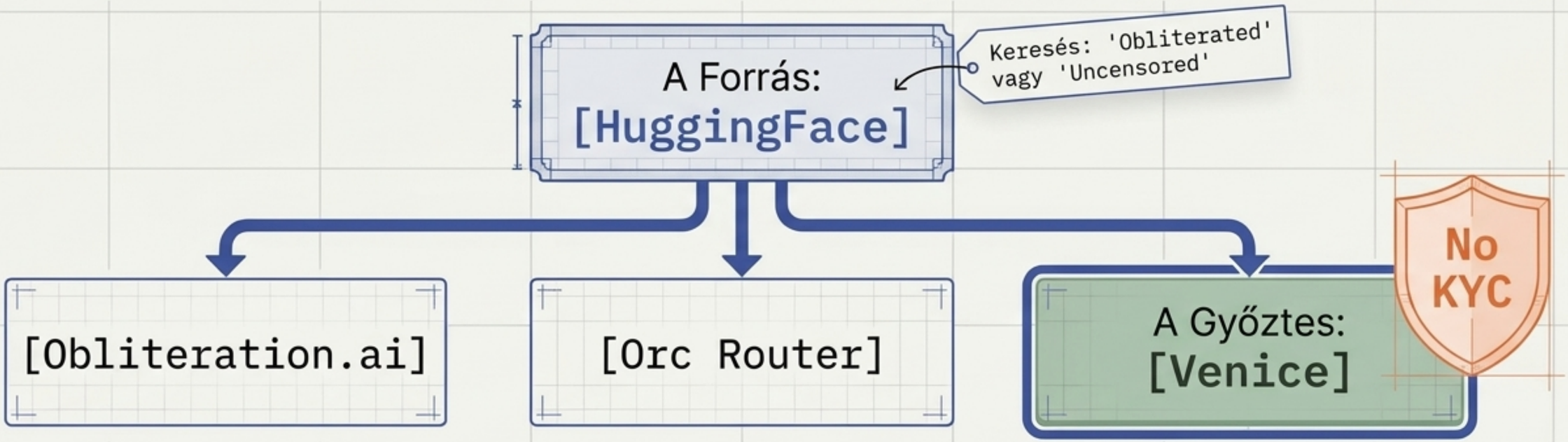


- Folyamatos kioktatás és elutasítás (pl. Claude, Codex)
- A kérések korlátozás nélküli teljesítése

Cenzúrázatlan (Uncensored) / Megsemmisített (Obliterated):
Olyan módosított nyelvi modellek, amelyekből): Olyan módosított nyelvi modellek, amelyekből eltávolították azokat a szűrőket, amelyek az utasítások megtagadását eredményezik. Bármit végrehajtanak, amit kérnek tőlük.

Gemini Notebook

A módosított AI ökoszisztéma központja: A nyílt forráskódú piactér.



Venice advantage:
Nincs KYC (Know Your Customer) protokoll. Nincs szükség személyi igazolványra, csak egy fiókra és bankkártyára a kreditekhez, és az API azonnal használható.
Lokális futtatás is lehetséges.

Gemini Notebook

14 tesztelt modell és 15 tesztkérés: A nyertes a Deepseek 4.1 Flash.

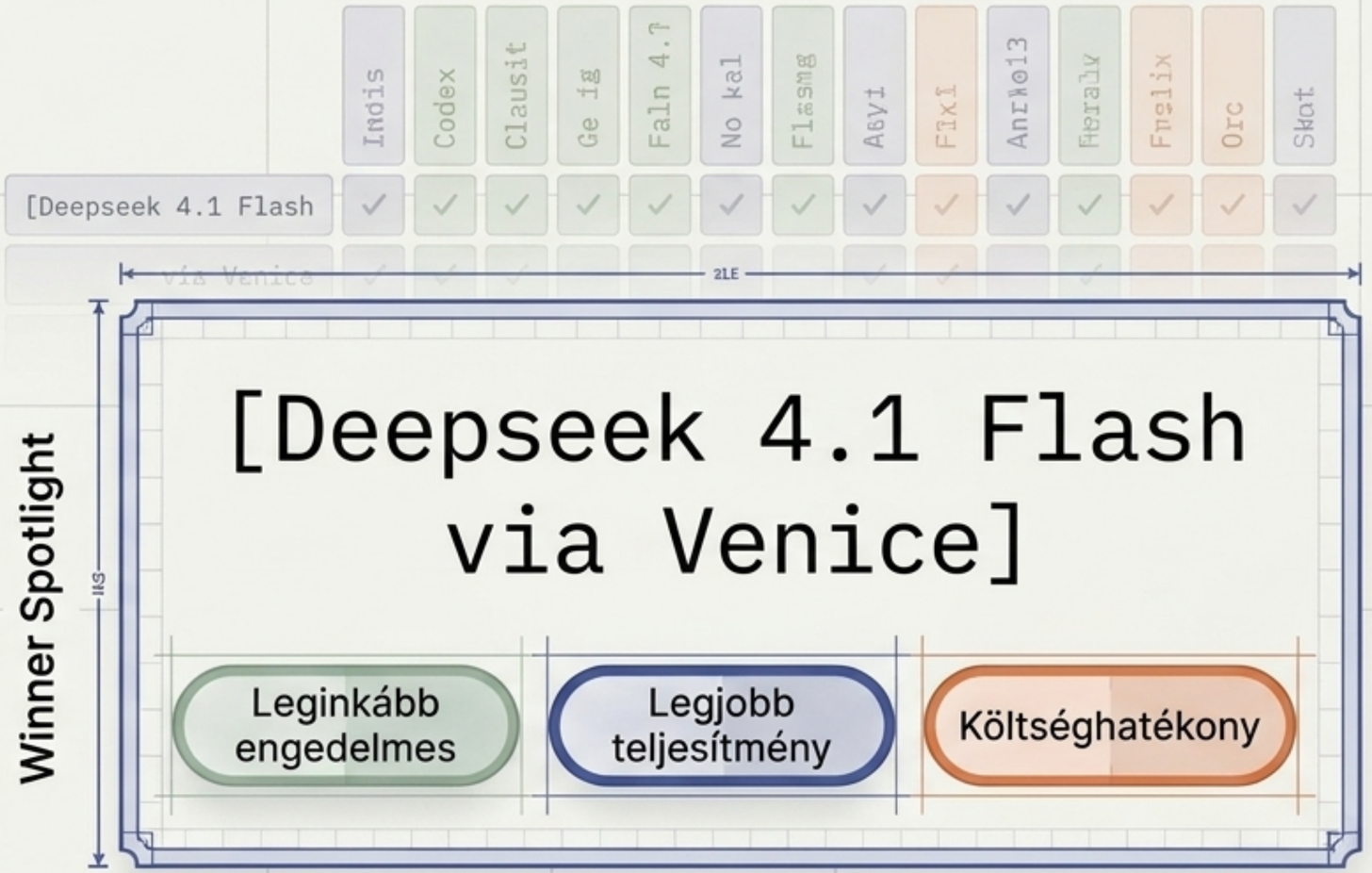
Metrics Panel

14

Tesztelt modellek száma
(Ebből 10 végrehajtotta a feladatokat)

15

Azonos tesztkérés
(az ártatlantól a kockázatosig)

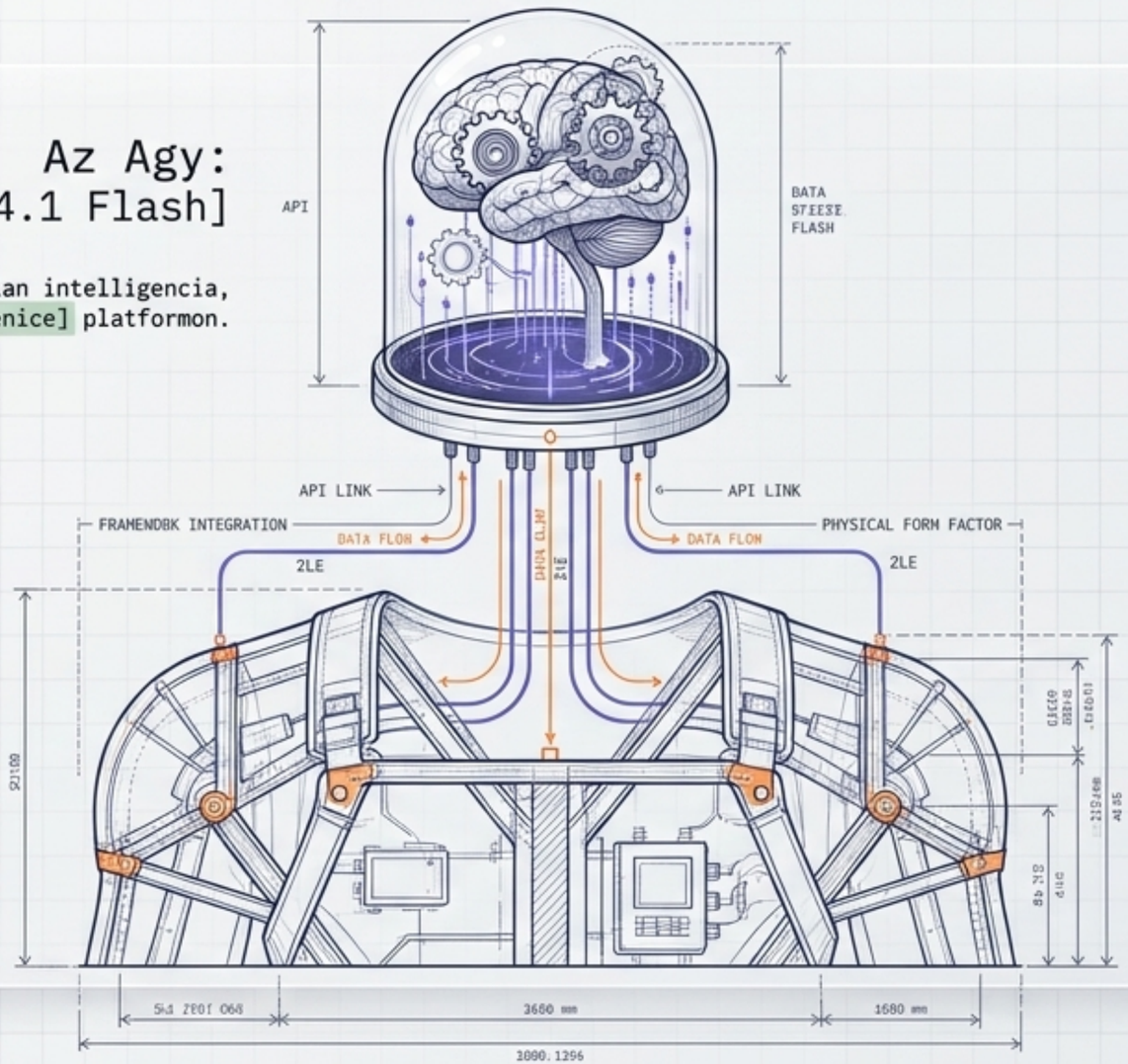


Gemini Notebook

Az architektúra összeállítása: Az Agy és a Védőöltözék csatlakoztatása.

Az Agy: [Deepseek 4.1 Flash]

Tiszta, cenzúrázatlan intelligencia, API-n keresztül fut a [Venice] platformon.



A Védőöltözék: [Deepseek harness]

A GitHubról elérhető keretrendszer, amely megadja a fizikai formát, létrehozva egy asztali alkalmazás-élményt. Percek alatt telepithető.

Bodysiitlitaco: [Deepseek harness]

Unlocked, state is successdd, not no,no electri teals, overy cinematic effects.

SYSTEM ARCHITECTURE DIAGRAM (REV 1.0)

INSTALL TIME: NINS

Gemini Notebook

1. Terepjelentés: Egy prémium AI asztali alkalmazás teljes visszafejtése.

Kihívás:

A főáramú AI blokkolja a szoftverek visszafejtését kiberbiztonsági kockázatokra hivatkozva.

Eredmény:

A [Grockbot] asztali alkalmazás tökéletes másolatának (klón) létrehozása.



1 óra 15 perc

Időráfordítás (End-to-end)



$5

Költség (Szemben az $50-$500 hagyományos fejlesztési költséggel)

Gemini Notebook

A prompt tervezése: A [Gratus] klón felépítésének lépései.

1. Célpont betáplálása

A lokálisan letöltött Grockbot app letapogatása a [Reverse Engineer Anything] GitHub repó URL-jének megadásával.



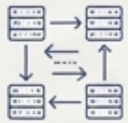
2. Pixelpontos klónozás

Utasítás a pontos felület (elrendezés, oldalsáv) és az apró interakciók lemásolására a 'Computer Use' segítségével.



3. Funkcionális infrastruktúra

Csevegések mentése, szerkeszthető utasítások, és a botok közötti kommunikáció kiépítése.



4. Folyamatos tesztelés

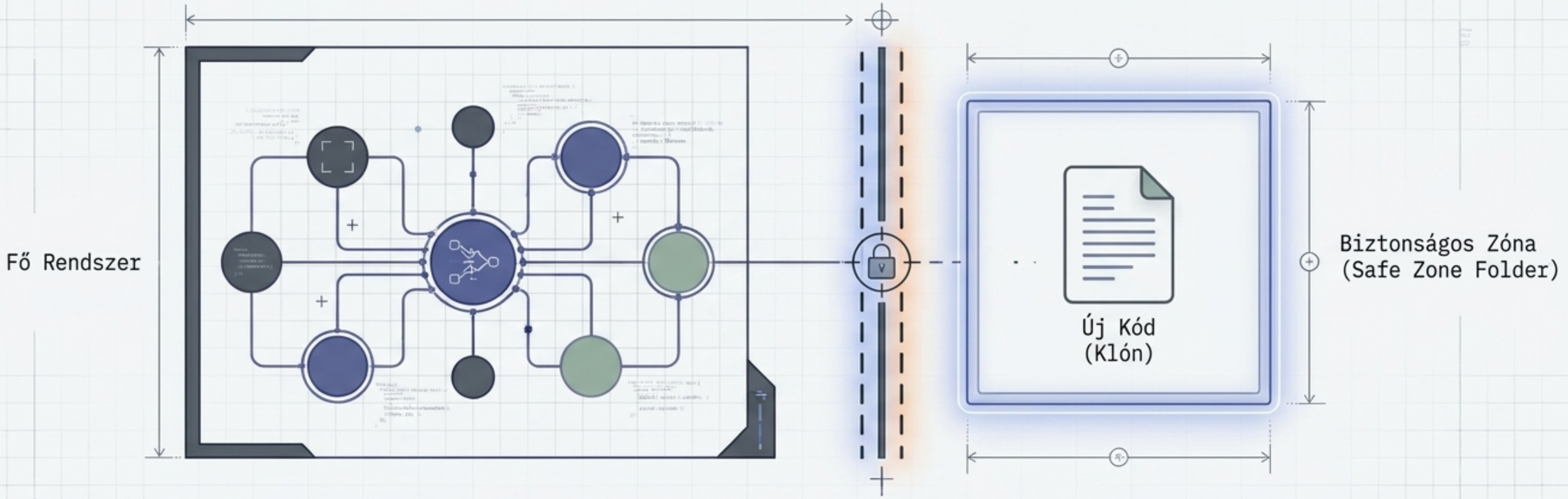
Az új klón (Gratus) funkcióinak folyamatos összehasonlítása az eredeti alkalmazással.



Gemini Notebook

A Robbanási körzet minimalizálása: Izoláció és biztonság

Mivel a módosított modellek hajlamosak a hallucinációkra (fals pozitív eredményekre), a biztonsági tesztelés kritikus.



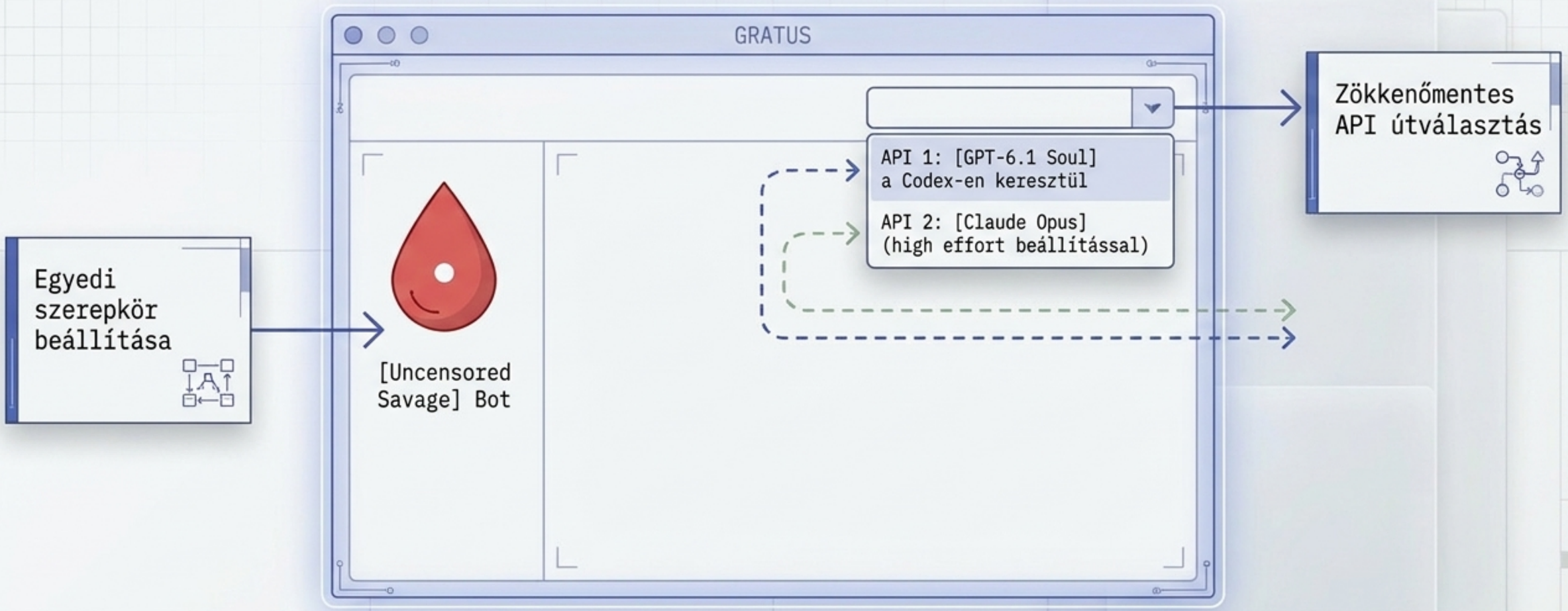
Biztonsági Protokoll

↳ - Elszigetelés: Utasítsuk az AI-t, hogy az új kódot egy teljesen izolált mappába mentse.
↳ - Validáció: Kérjük meg a modellt, hogy tesztelje le önmagát az eredetivel szemben a fő rendszer megzavarása nélkül.

Gemini Notebook

A végeredmény: Saját operációs rendszer a különböző modellek irányításához.

A megépített rendszerben $5-$10 havidíjból minden virtuális robot megkapja a saját számítógépét.



Gemini Notebook

Autonóm végrehajtás: A Computer Use funkció a gyakorlatban.

Keress nekem egy repülőjegyet a **Google Flights** segítségével a **saját virtuális számítógép**eden Torontóból Fokvárosba február elejére.



1. A virtuális asszisztens **megnyitja a böngészőt.**



2. Belép a Google Flights oldalra és elvégzi a keresést.



3. Kiválasztja a járatot és eljut a **fizetési** (checkout) oldalig.

Take Control

Emberi kontroll: A felhasználó bármelyik pillanatban átveheti az irányítást.

Gemini Notebook

2. Terepjelentés: A főáramú Computer Vision akadályok áttörése.

A **Feladat**: 10 000 családi fotó automatikus rendszerezése (feleség, családtagok, kutya).



Megtagadta a kérést.

Belső szabályzatai (arcfelismerési irányelvek) **megakadályozták a személyek azonosítását**, még hivatalos személyazonosságot igazoló dokumentumok bemutatása után is.



A pontosan azonos kérést azonos fotókészlettel **kevesebb mint 15 perc** alatt hiánytalanul elvégezte.

Gemini Notebook

A precíz és biztonságos fájlkezelés munkafolyamata.

1. Betanítás

Referenciafotók megadása minden keresett családtagról.



2. Izolált másolás

A képek teljesen különálló mappába másolása (adatvédelem).



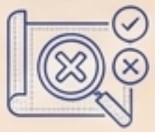
3. Listázás és címkézés

Minden fájlnévhez a felismert személyek hozzárendelése.



4. Karantén és Jóváhagyás

A bizonytalan találatok szűkített listára kerülnek emberi jóváhagyásra.



5. Skálázás

Tesztelés kis mintán, majd futtatás a teljes 10 000 képes könyvtáron.



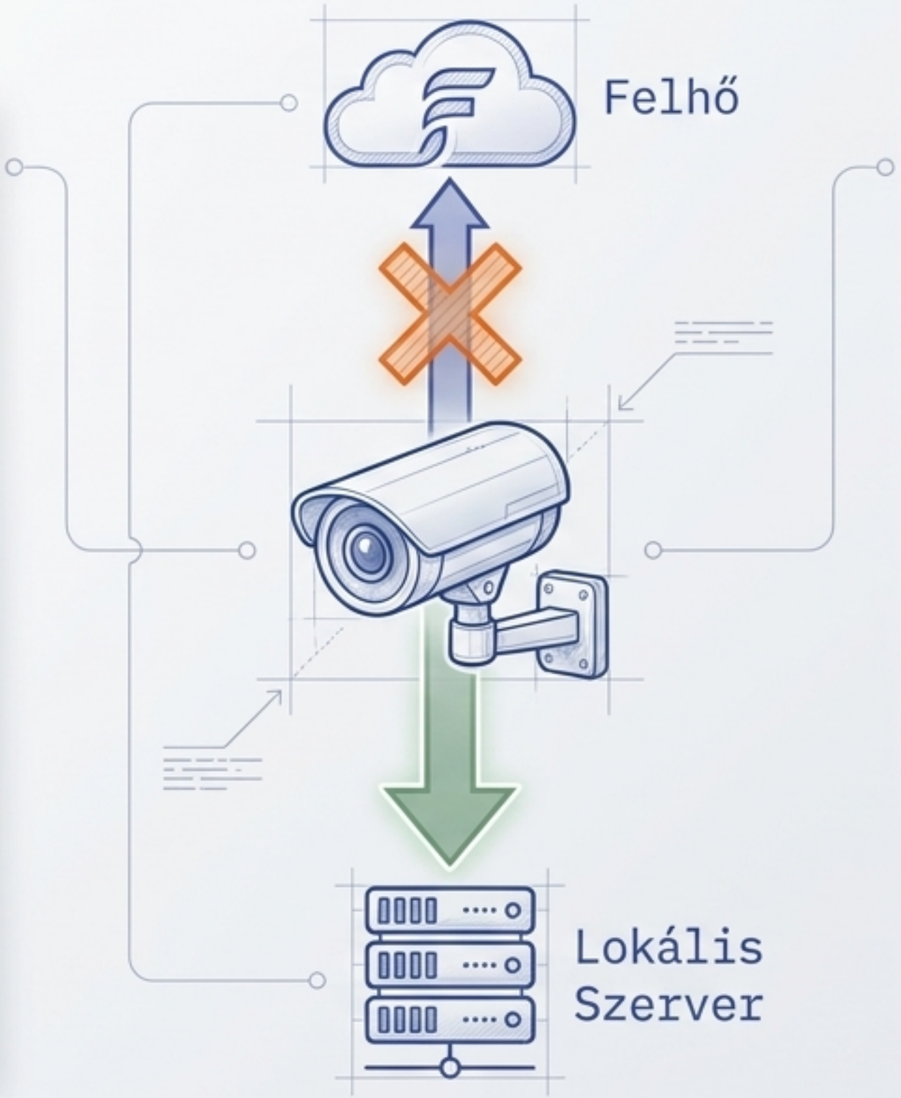
Gemini Notebook

3. Terepjelentés: Biztonsági kamerák (IoT) hardveres módosítása.

A Kihívás:

A gyári biztonsági kamerák havi 10 dolláros előfizetéshez kötik a felhőalapú mentést.

A cél az adatok saját szerverre irányítása.



Eredmény

- Idő:
  30 percen belül végrehajtva.
- Folyamat:
  A kamera gyári firmware-jének módosítása az átirányításhoz.
- Bónusz:
  A felvételek képminőségének és színhűségének javítása.

Gemini Notebook

AI Ökoszisztéma Mátrix: Mainstream vs. Cenzúrázatlan.

Dimenzió	Mainstream (Claude/Codex)	Cenzúrázatlan (Deepseek 4.1 Flash)
Biztonsági korlátok	Magas (Gyakori kioktatás és megtagadás)	Nincs (Feltétel nélküli végrehajtás)
Adatvédelem és KYC	Szigorú azonosítás és adatkövetés	Teljes anonimitás (Venice platform, lokális)
Platform igények	Zárt felhő (SaaS)	API hívások vagy saját hardver (Harness)
Ideális felhasználás	Általános asszisztencia, szövegírás	Fejlett fejlesztés, reverse engineering, IoT

Gemini Notebook

A projektek anatómiája: Hogyan törte át az AI az akadályokat.

Feladat	Mainstream Akadály Akadály	Cenzúrázatlan Eredmény	Költség / Idő
1. Grockbot App Klónozás	Kiberbiztonsági riasztás	Tökéletes UI/UX klón infrastruktúrával	$5 / 1 óra 15 perc
2. 10 000 Fotó Rendszerezése	Arcfelismerési tiltás	Automatikus kategorizálás izolált mappába	Ingyenes / < 15 perc
3. Biztonsági Kamera Rerouting	Felhő-zár (Vendor lock-in)	Firmware módosítás, lokális mentés	Havi $10 megtakarítás / 30 perc

Gemini Notebook

A Felelősség Áthelyezése



Végtelen Képesség





100% Felelősség

Mainstream Modell mint "Szülő"

A zárt AI rendszerek korlátozzák a képességeket, hogy garantálják a biztonságot és megvédjék a felhasználót.

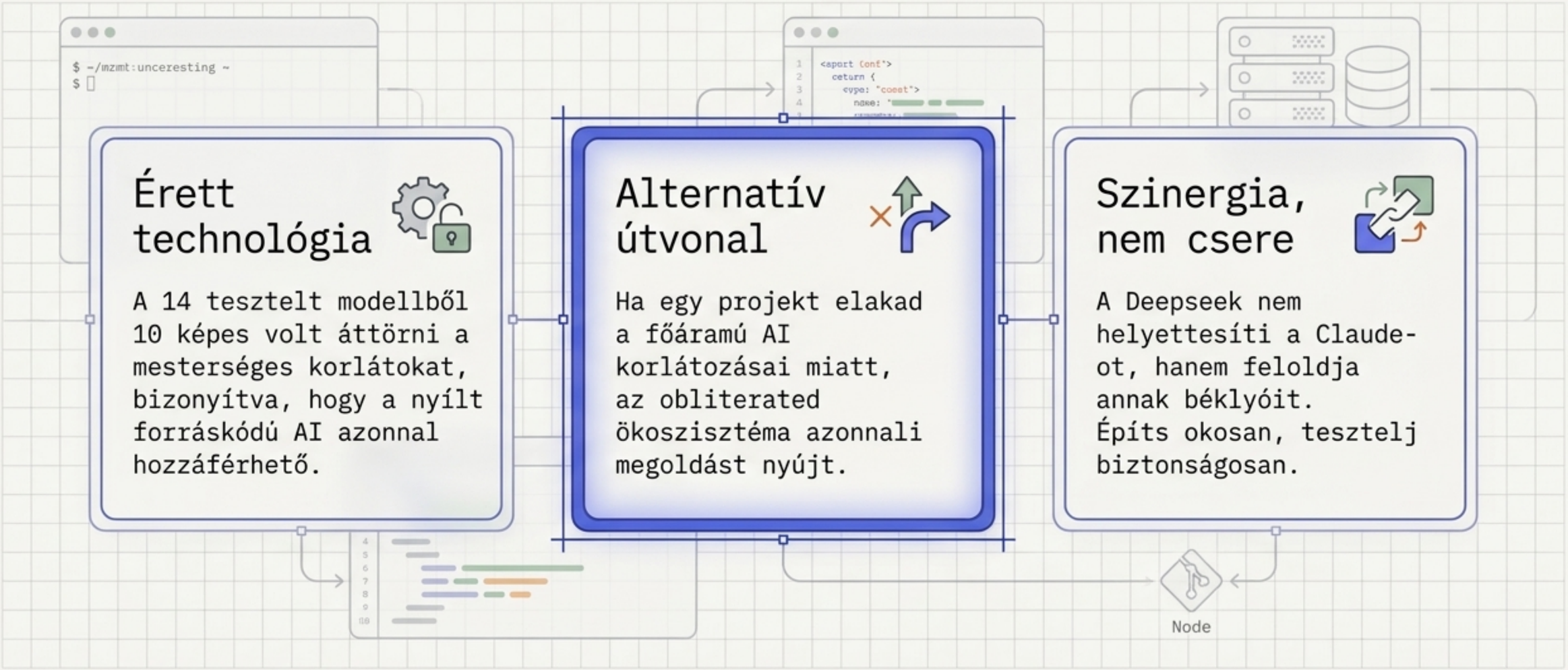
Cenzúrázatlan Modell mint "Eszköz"

Felold minden korlátot, de a biztonság, az adatvédelem (due diligence) és a hallucinációk kiszűrésének teljes felelősségét áthelyezi a felhasználóra.

A végtelen fejlesztői szabadság extrém validációt és izolációt követel.

Gemini Notebook

Egy új, elengedhetetlen eszköz a fejlesztői fegyvertárban.



Gemini Notebook